UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/626,185	07/24/2003	Mira Kristina LaCous	S30.12-0006	1550

27367 7590 07/30/2007
WESTMAN CHAMPLIN & KELLY, P.A.
SUITE 1400
900 SECOND AVENUE SOUTH
MINNEAPOLIS, MN 55402-3319

EXAMINER	
GERGISO, TECHANE	
ART UNIT	**PAPER NUMBER**
2137	
MAIL DATE	**DELIVERY MODE**
07/30/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/626,185	**Applicant(s)** LACOUS, MIRA KRISTINA	
	Examiner Techane J. Gergiso T-G	**Art Unit** 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 April 2007*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-49* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-49* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. This in a Final Office Action in response to the applicant's communication filed on April 13, 2007.

2. Claims 1-48 have been examined and claims 1-48 are pending.

Response to Arguments

3. Applicant's arguments filed on April 13, 2007 have been fully considered but they are not persuasive.

4. Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.

The applicant argues, fore example, "The section does not disclose transmitting a session packet, or anything else, to the biometric device (292) as is recited in claim 1."

The examiner disagrees with the applicant's argument because Gould et al. teaches in column 5: lines 9-31 recited as follows. " FIG. 4 is a flow chart which illustrates the connectivity of the above-identified functions in accordance with the present invention. FIG. 5 is a diagram which illustrates the method of operation of biometric capture device 292 within a client 104 and alert operations within server 100 in accordance with the present invention. (22) Referring to FIGS. 4 and 5 together, first, a user presents the appropriate biometric input such as fingerprint, retina, voice, or handwriting to the biometric device (i.e., USB device 292) at the client 104, via step 402. Next, the client 104 conditions the biometric data into an appropriate template format, via step 404. The client 104 then signs and encrypts this template using the client unique platform private key and server public key, via step 406. **Then the client 104 sends this data to a server 100, via step 408.** The server 100 verifies that the data is from an authorized client in its enterprise by using a client platform public key and server private key to decrypt and verify the signature and message, via step 410. Then the server 100 uses the verified and decrypted biometric data and matches it against previously enrolled templates, via step 412. These templates would typically have been captured during initial employee enrollment into the enterprise (i.e., when initially badged or granted access privileges).

Next, the server 100 pulls from a secure database the appropriate authentication credentials for the biometric identified user and encrypts them using the client platform public key and server private key, via step 414. The server 100 then signs this data using the server private key, via step 416. **At this point the server 100 sends this data to the client 104, via step 418.** The client 104 accepts and verifies that the data is from the server 100 using the server public key, via step 420. The client 100 then decrypts the data using the client private key, via step 422. The client 104 installs user credentials into appropriate devices and services, via step 424.“ The examiner disagrees with the applicant because at least the emphasized section shows the communication between the client with biometric and server.

The applicant also argues “The process described in Gould figure 4: 420-426 first makes a determination of whether or not to utilize the data (Gould figure 4: 420) before it decrypts the data (Gould figure 4: 422). This is a different process than that of claim 1, which very generally speaking, decrypts the data and then makes a determination as to whether or not to utilize the data.

The examiner disagrees with the applicant's argument because the applicant did not specifically claimed as his invention the sequence or order of the processes as argued in the remark.

5. Therefore the applicant's argument is not persuasive to overcome Gould et al. in view of Michener et al. to place independent claims 1, 23, 27 and 35 in condition for allowance for at least the above given reasons. The applicant's argument is not also not persuasive to overcome the prior arts in record to place dependant claims 2-22, 24-26, 28-34 and 36-48 depending directly or indirectly from their corresponding independent claims to place them in condition for allowance for the above given reasons.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1-48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gould et al. (hereinafter referred to as Gould, US Pat. No.: 6, 920, 561) in view of Michener et al. (hereinafter referred to as Michener, US Pat. No. 7, 028, 191).

As per claim 1:

Gould discloses a computer-implemented method for enhancing the security of informational interactions with a biometric device, comprising:

pre-establishing an encryption relationship between a computing device and the biometric device (column 1: lines 50-66; figure 3: Associate biometric input and credential on server; figure 4; column 5: lines 9-31);

generating a session packet, and transmitting it to the biometric device (figure 4: Server Pulls from a secure database the appropriate authentication credentials for the biometric identified user; Server signs this data using the server private key; Server, sends this data to the client; column 5: lines 9-31); and

receiving a biometric information packet, decrypting it, and making a determination, based on a content of a collection of information contained in the decrypted biometric information packet, as to whether or not to utilize a collection of biometric data contained in the decrypted biometric information packet (figure 4: 420-426; The server encrypts the bio, pulls associate credentials from a secure database, encrypts the credentials and sends to the client. The method further comprises the client accepting and verifying credentials associated with the signed and encrypted data from the server utilizing the public key from the server. The method further comprises installing the credentials into the computer if the credentials are verified. (Column 5: lines 9-31).

Gould does not explicitly teach encrypting the generated session packet. Michener, in an analogous art, however teaches encrypting the generated session packet (column 4: lines 55-67; column 5: lines 40-67; figure 5a, 5b; column 7: lines 15-60). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Gould to include encrypting the generated session packet. This modification would have been obvious because a person having ordinary skill in the art would have been motivated by the desire a personal protection of electronic data that is small, easy to use, provides excellent protection to the PC/laptop use, that can operate in conjunction with corresponding devices at a central data gathering point to provide near real time validation of the information as suggested by Michener (in column 2: lines 55-62).

As per claim 2:

Michener discloses a method, wherein generating a session packet comprises generating a session number and storing it in the session packet (column 9: lines 5-40; Session-Random Number; Figure 1: 16; 50).

As per claim 3:

Michener discloses a method, further comprising storing the session number in a database associated with the computing device (Column 4: lines 52-65; Each TAD 10 is provided with a unique alphanumeric ID (TADID_A) and a unique and well-protected binary ID (TADID_B), each of which are stored in memory 26. Column 10: lines 1-25; figure 13: Table Lookup; data structure).

As per claim 4:

Michener discloses a method, wherein generating a session packet comprises obtaining a session key and storing it in the session packet (column 7: lines 10-30; column 9: lines 1-30).

As per claim 5:

Michener discloses a method, further comprising storing the session key in a database associated with the computer (Column 10: lines 1-25; figure 13: Table Lookup; data structure).

As per claim 6:

Michener discloses a method, wherein receiving a biometric information packet and decrypting it comprises receiving a biometric information packet and decrypting it with an encryption key that is complimentarily related to the session key (figure 10: 104, 1008, 1010; column 13: 54-65; column 15: lines 5-10, lines 16-23).

As per claim 7:

Michener discloses a method, wherein obtaining a session key comprises generating a public key portion of a PKI key pair (column 17: lines 5-11).

As per claim 8:

Michener discloses a method, wherein receiving a biometric information packet and decrypting it comprises receiving a biometric information packet and decrypting it with a private key portion of the PKI key pair (column 17: lines 5-11).

As per claim 9:

Michener discloses a method, wherein receiving a biometric information packet and decrypting it comprises receiving a biometric information packet and decrypting it with an encryption component that is independent of the pre-established encryption relationship (figure 17).

As per claim 10:

Michener discloses a method, wherein generating a session packet comprises generating a session time stamp and storing it in the session packet (figure 13).

As per claim 11:

Michener discloses a method, wherein generating a session packet comprises: generating a session number and storing it in the session packet; and obtaining a session key and storing it in the session packet (figure 170.

As pr claim 12:

Michener discloses a method, further comprising storing the session number, the session key and a session time stamp in a database associated with the computer (figure 17).

As per claim 13:

Michener discloses a method, wherein making a determination comprises comparing a session number to a list of valid values (column 9: lines 5-35).

As per claim 14:

Michener discloses a method, wherein making a determination comprises evaluating a session time stamp to determine whether the biometric information packet was received within a predetermined time period (column 2: lines 55-60; figure 17).

As per claim 15:

Michener discloses a method, wherein making a determination comprises comparing a data representation of a user's biometric information to at least one data representation of biometric information stored in a database (column 5: lines 20-40).

As per claim 16:

Michener discloses a method, wherein making a determination comprises: comparing a session number to a list of valid values (column 9: lines 5-35); evaluating a session time stamp to determine whether the biometric information packet was received within a predetermined time period (column 2: lines 55-60; figure 17); and comparing a database representation of a user's biometric information to at least one data representation of biometric information stored in a database (figure 17; column 9: lines 5-35; column 5: lines 20-40).

As per claim 17:

Michener discloses a method, wherein pre-establishing an encryption relationship comprises storing a first encryption component with the computing device and a second encryption component with the biometric device, one of the first and second encryption components being configured to decrypt information that has previously been encrypted utilizing the other of the first and second encryption components (figure 8: 802-808; figure 10: 1002-1012; abstract).

AS per claim 18:

Michener discloses a method, wherein encrypting the session packet comprises encrypting the session packet utilizing one of the first and second encryption components (figure 10: 1002-1022; abstract).

As per claim 19:

Michener discloses a method, wherein pre-establishing an encryption relationship comprises storing a first part of a PKI key pair with the computing device and a second part of the PKI key pair with the biometric device (figure 10: 1002-1022; abstract).

As per claim 20:

Michener discloses a method, wherein encrypting the session packet comprises encrypting the session packet utilizing one of the first and second parts of the PKI key pair (figure 10: 1002-1022; abstract).

As per claim 21:

Michener discloses a method, wherein pre-establishing an encryption relationship comprises storing a first part of a static encryption key pair with the computing and a second part of the static encryption key pair with the biometric device, one of the first and second parts being configured to decrypt information that has previously been encrypted utilizing the other part (figure 10: 1002-1022; abstract).

As per claim 22:

Michener discloses a method, wherein encrypting the session packet comprises encrypting the session packet utilizing one of the first and second parts of the static encryption key pair (figure 10: 1002-1022; abstract).

As per claim 23:

Gould discloses a data packet for transmission from a computer to a biometric device during a process of authentication within a biometric security system, the data packet comprising (Preamble is not given patentable weight):

a session key, the session key configured to be utilized to encrypt data (column 1: lines 50-66; figure 3: 302-302; figure 4; (figure 4: 414-418); figure 3: 420-426).

Gould does not explicitly teach encrypting the generated session packet. Michener, in an analogous art, however teaches encrypting the generated session packet (column 4: lines 55-67; column 5: lines 40-67; figure 5a, 5b; column 7: lines 15-60). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Gould to include encrypting the generated session packet. This modification would have been obvious because a person having ordinary skill in the art would have been motivated by the desire a personal protection of electronic data that is small, easy to use, provides excellent protection to the PC/laptop use, that can operate in conjunction with corresponding devices at a central data gathering point to provide near real time validation of the information as suggested by Michener (in column 2: lines 55-62).

As per claim 24:

Michener discloses a method, wherein the session key is a public key portion of a PKI key pair (column 17: lines 5-11).

As per claim 25:

Michener discloses a method, further comprising a session number (Column 10: lines 1-25; figure 13: Table Lookup; data structure).

As per claim 26:

Michener discloses a method, wherein the session number is a value that corresponds to a session initiated when the data packet is generated (figure 8: initiate transaction on client computer; TADID_ Data Structure).

As per claim 27:

Gould discloses a biometric device configured to support a secure transfer of biometric information to a computing device, the biometric device comprising:

a biometric information receiver configured to capture an individual's biometric information (figure 3: 308); figure 5: 292;

a processor configured to process the biometric information and produce a digitized representation thereof (column 1: lines 50-66; figure 3: 302-302; figure 4);

a memory accessibly connected to the processor (figure 2: 206); and

an encryption component stored in the memory, the processor being configured to receive an encrypted session packet from the computing device and decrypt it utilizing the encryption component (figure 3: 420-426; column 1: lines 50-66; figure 3: 302-302; figure 4).

Gould does not explicitly teach encrypting the generated session packet. Michener, in an analogous art, however teaches encrypting the generated session packet (column 4: lines 55-67; column 5: lines 40-67; figure 5a, 5b; column 7: lines 15-60). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Gould to include encrypting the generated session packet. This modification would have been obvious because a person having ordinary skill in the art would have been motivated by the desire a personal protection of electronic data that is small, easy to use, provides excellent protection to the PC/laptop use, that can operate in conjunction with corresponding devices at a central data gathering point to provide near real time validation of the information as suggested by Michener (in column 2: lines 55-62).

As per claim 28:

Michener discloses a biometric device, wherein the encryption component is implemented as firmware (column 7: lines 11-52).

As per claim 29:

Gould discloses a biometric device, wherein the encryption component is implemented in association with a flash memory application (column 3: 25-30).

As per claim 30:

Michener discloses a biometric device, wherein the encryption component is one part of a PKI key pair (column 17: lines 5-11).

As per claim 31:

Michener discloses a biometric device, wherein the encryption component is one part of a static encryption key pair (column 17: lines 5-11).

As per claim 32:

Michener discloses a biometric device, wherein the processor is further configured to place the digitized representation into a biometric information packet (column 4: lines 55-67; column 5: lines 40-67; figure 5a, 5b; column 7: lines 15-60).

As per claim 33:

Michener discloses a biometric device, wherein the processor is further configured to encrypt the biometric information packet utilizing a specialized encryption component contained in the session packet (column 4: lines 55-67; column 5: lines 40-67; figure 5a, 5b; column 7: lines 15-60).

As per claim 34:

Michener discloses a biometric device, wherein the processor is further configured to transfer the encrypted biometric information packet to the computer (figure 10: 1002-1022; abstract).

As per claim 35:

Gould discloses a computer readable medium having instructions stored thereon which, when executed by a computing device, cause the computing device to perform a series of steps comprising:

receiving a session initiation command (figure 3: 302);

generating a session packet (figure 4: 414-418);

transmitting the encrypted session packet to a biometric device (column 5: lines 32-45);

receiving a biometric information packet from the biometric device (column 5: lines 14-28);

decrypting the biometric information packet (column 5: lines 32-45); and

determining, based on a content of a collection of authentication information contained in the decrypted biometric information packet, whether or not to utilize a collection of biometric data contained in the decrypted biometric information packet (figure 3: 420-426).

Gould does not explicitly teach encrypting the generated session packet. Michener, in an analogous art, however teaches encrypting the generated session packet (column 4: lines 55-67; column 5: lines 40-67; figure 5a, 5b; column 7: lines 15-60). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Gould to include encrypting the generated session packet. This modification would have been obvious because a person having ordinary skill in the art would have been motivated by the desire a personal protection of electronic data that is small, easy to use, provides excellent protection to the PC/laptop use, that can operate in conjunction with corresponding devices at a central data gathering point to provide near real time validation of the information as suggested by Michener (in column 2: lines 55-62).

As per claim 36:

Michener discloses a computer readable medium, wherein generating a session packet comprises generating a session number and storing it in the session packet (column 9: lines 5-40; Session-Random Number).

As per claim 37:

Michener discloses a computer readable medium, further comprising the step of storing the session number in a database associated with the computing device (Column 10: lines 1-25; figure 13: Table Lookup; data structure).

As per claim 38:

Michener discloses a computer readable medium, wherein generating a session packet comprises obtaining a session key and storing it in the session packet (column 7: lines 10-30; column 9: lines 1-30).

As per claim 39:

Michener discloses a computer readable medium, further comprising the step of storing the session key in a database associated with the computer (Column 10: lines 1-25; figure 13: Table Lookup; data structure).

As per claim 40:

Michener discloses a computer readable medium, wherein receiving a biometric information packet and decrypting it comprises receiving a biometric information packet and decrypting it with an encryption key that is complimentarily related to the session key (figure 10: 104, 1008, 1010; column 13: 54-65; column 15: lines 5-10, lines 16-23).

As per claim 41:

Michener discloses a computer readable medium, wherein obtaining a session key comprises generating a public key portion of a PKI key pair (column 17: lines 5-11).

As per claim 42:

Michener discloses a computer readable medium, wherein receiving a biometric information packet and decrypting it comprises receiving a biometric information packet and decrypting it with a private key portion of the PKI key pair (column 17: lines 5-11).

As per claim 43:

Michener discloses a computer readable medium, wherein generating a session packet comprises generating a session time stamp and storing it in the session packet (figure 13).

As per claim 44:

Michener discloses a computer readable medium, wherein determining comprises comparing a session number to a list of valid values (column 9: lines 5-35).

As per claim 45:

Michener discloses a computer readable medium, wherein determining comprises evaluating a session time stamp to determine whether the biometric information packet was received within a predetermined time period (column 2: lines 15-60; figure 17).

As per claim 46:

Michener discloses a computer readable medium, wherein encrypting the session packet comprises encryption the session packet with a first encryption component that is complimentarily related to a second encryption component maintained on the biometric device, one of the first and second encryption components being configured to decrypt information that has previously been encrypted utilizing the other of the first and second encryption components (figure 8: 802-808; figure 10: 1002-1012; abstract).

As per claim 47:

Michener discloses a computer readable medium, wherein the first and second encryption components are a PKI key pair (figure 10: 1002-1022; abstract).

As per claim 48:

Michener discloses a computer readable medium, wherein the first and second encryption components are a static encryption key pair (figure 10: 1002-1022; abstract).

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

See the notice of reference cited in form PTO-892 for additional prior art.

9. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Contact Information

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Techane J. Gergiso whose telephone number is (571) 272-3784 and fax number is (571) 273-3784. The examiner can normally be reached on 9:00am - 6:00pm. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor,

Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

T-G
Techane Gergiso
Patent Examiner
Art Unit 2137

July 22, 2007

Matthew B. Smithers
MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137